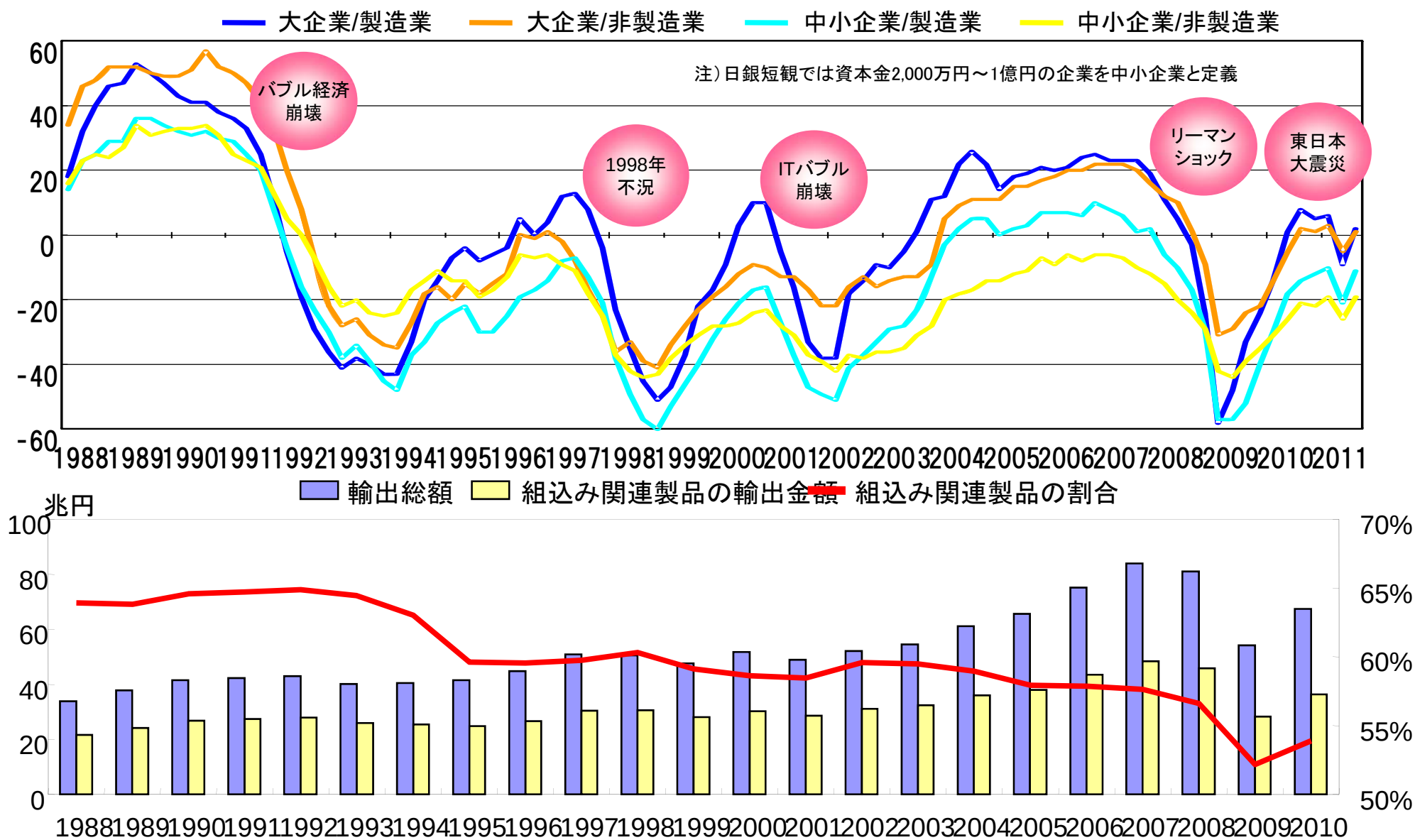


ソフトウェア品質監査制度(仮称)とトレーサビリティについて ～第三者の検証・妥当性確認による品質説明力の強化～

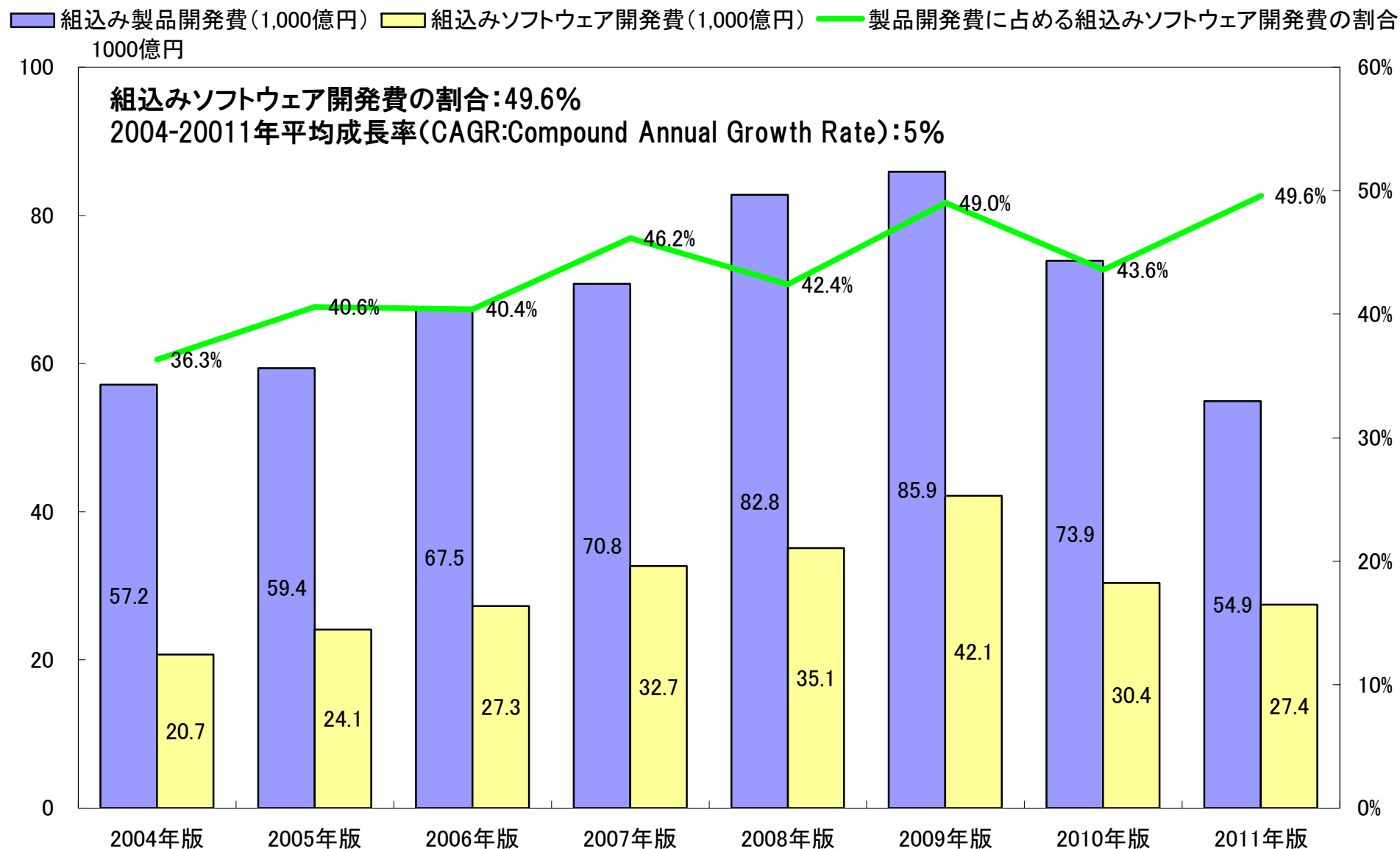
独立行政法人 情報処理推進機構 ソフトウェア・エンジニアリング・センター
統合系プロジェクト&組込み系プロジェクト サブリーダー

工学博士 田丸 喜一郎

日銀短観(1988年3月～2011年9月:四半期毎)と輸出金額の推移(1988年～2010年暦年)

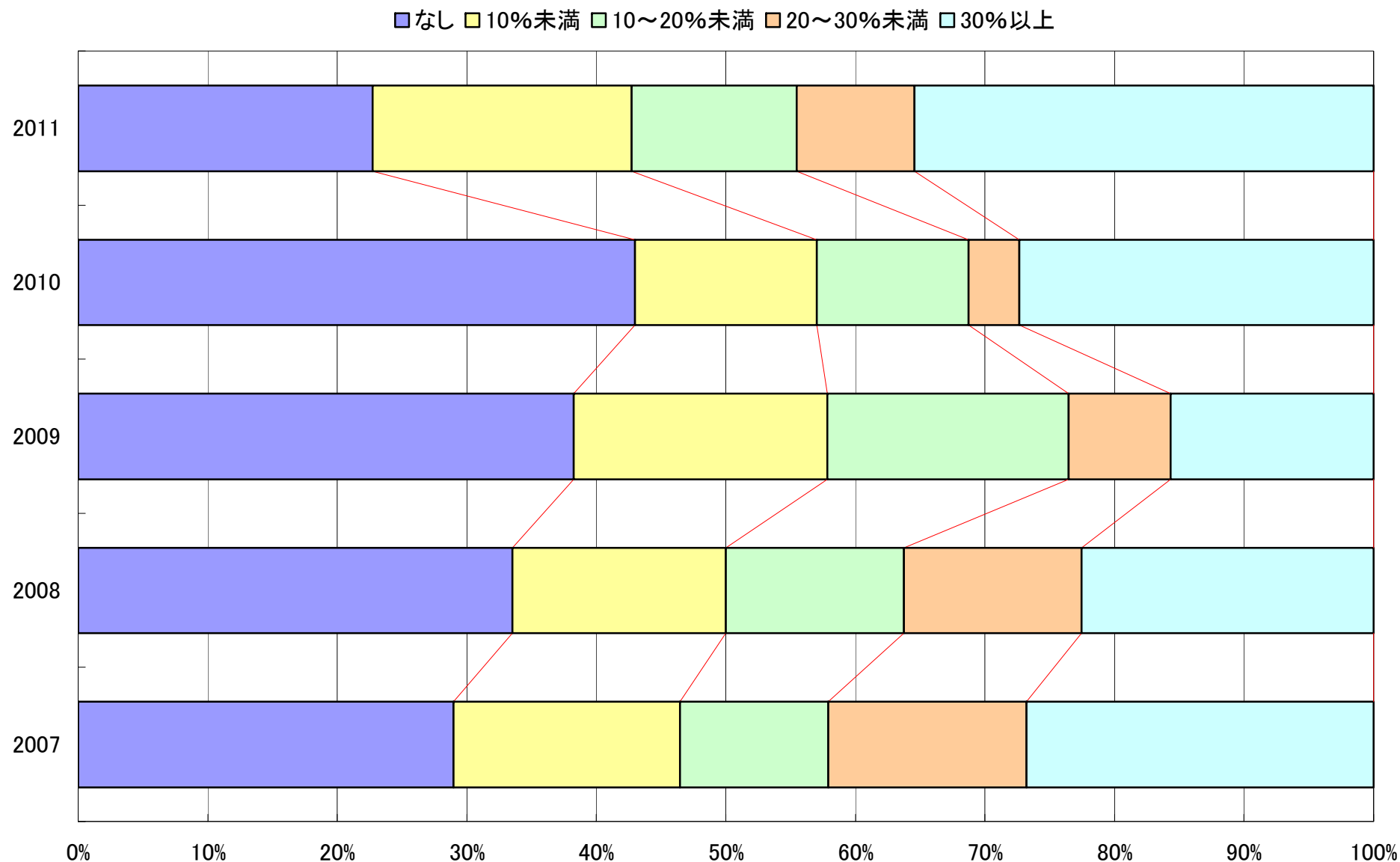


組込みシステム製品開発費と組込みソフトウェア開発費・開発費比率の推移



(社)日本機械工業連合会(平成21年度生産額実績統計)、組込みシステム産業の実態把握調査

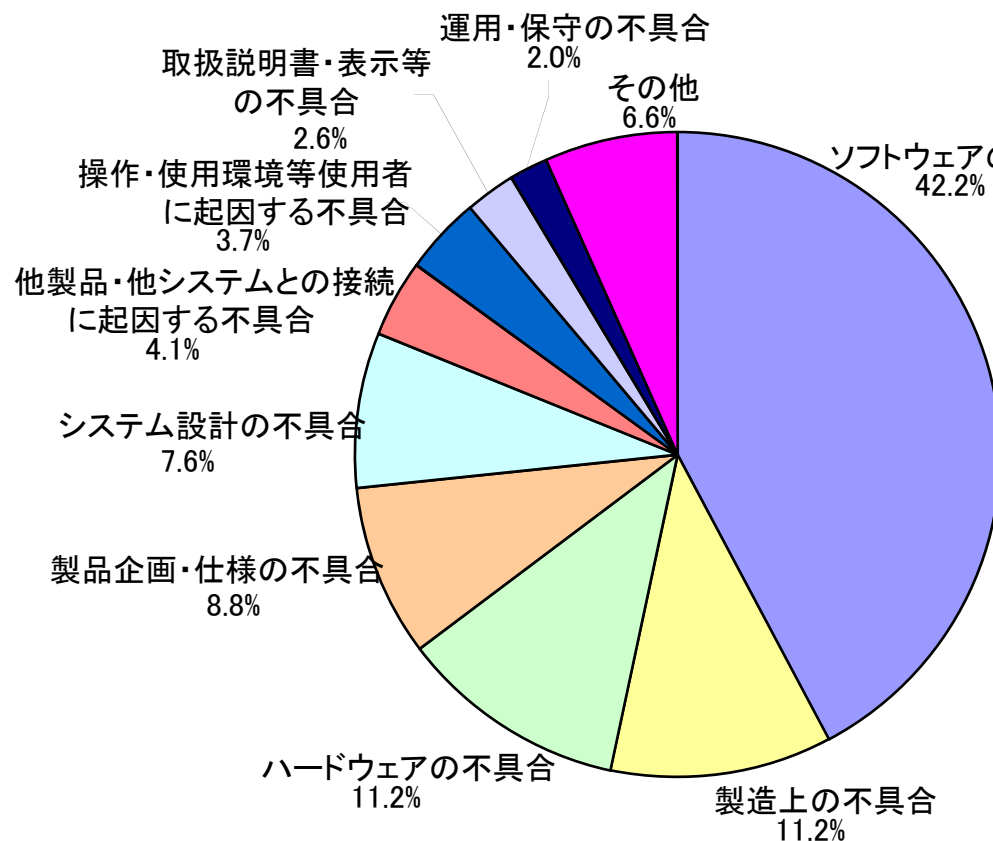
製品出荷後の不具合発生製品率の推移



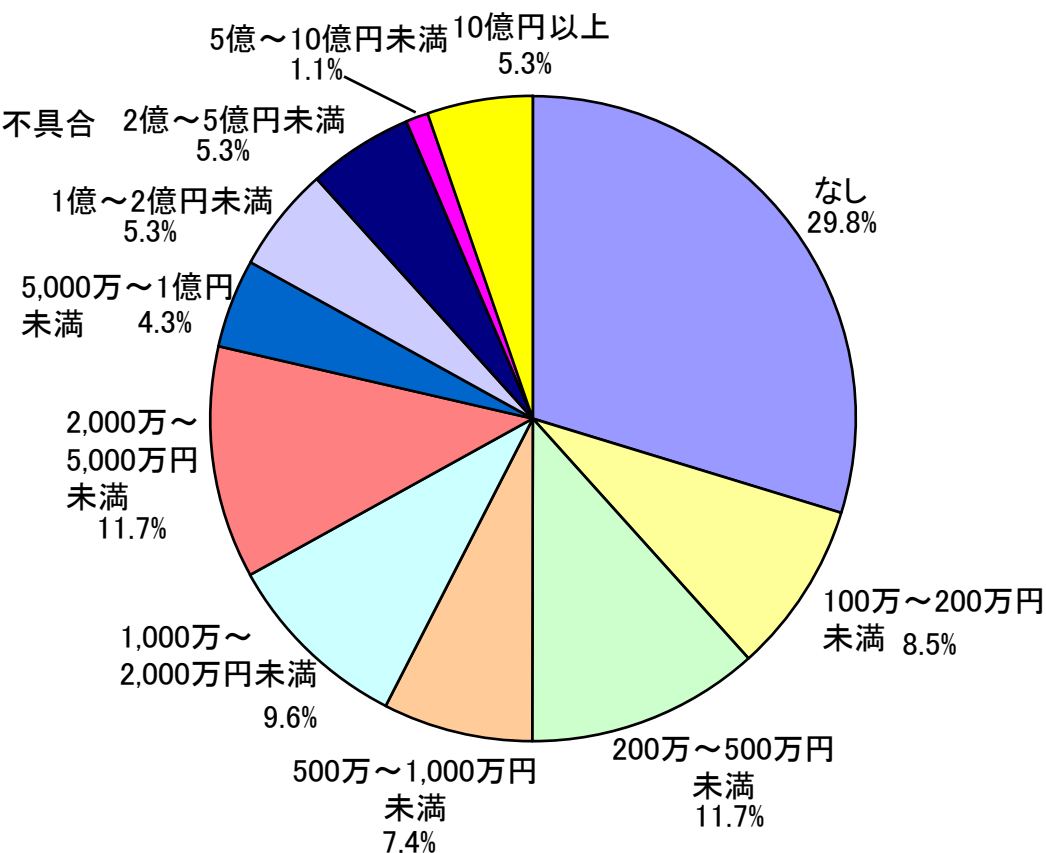
出典:「経済産業省 平成22年度 組込みシステム産業の実態把握調査」

製品出荷後の不具合の原因と「対策費＋損失」

不具合の原因(製品数ベース)



「対策費＋損失」



出典:「経済産業省 平成22年度 組込みシステム産業の実態把握調査」

組込みソフトウェア開発を取巻く事業環境の変化(1)

- 機能安全、第三者検証・妥当性確認など品質説明力の向上
 - 機能安全規格と第三者検証・妥当性確認の両者に対応した組込みソフトウェア開発（組込みソフトウェア開発に関わる全ステークホルダの対応が必要）
 - 対応した開発情報管理
 - 開発情報のトレーサビリティの確保
 - 開発に関わる技術活動記録、組織活動記録などのエビデンス収集
 - 開発に使用する開発ツールの認証取得
 - 説明力(証明力)の高い開発技術の適用
 - 形式手法、モデルベース手法など
- 実装中心から設計中心のソフトウェア開発への移行
 - 実装工程の海外アウトソースと機械化(自動コード生成ツール)の拡大により国内の開発は上流工程中心に移行
 - 上流工程の中核技術はモデルベース(モデル駆動)開発技術
 - 開発プロセスのモデルベース開発への適応(上流工程での設計検証など)
 - 開発ツール等の導入(モデルベース開発技術はツール支援を前提とした開発技術)
 - モデルベース開発技術を扱える上流工程技術者の育成
 - 基礎的な学力(数学、論理学など)が不足しているソフトウェア技術者の育成
 - 利用者情報、利用情報の活用
 - 要求獲得、要件定義、...

組込みソフトウェア開発を取巻く事業環境の変化(2)

■ 組込みシステムのおシステムとの統合化(統合システム化)

- 自動車の例:車載システムの統合化と並行して、車外システムとの統合化が進行
 - 電動機の採用による、スマートエネルギーシステムと統合化
 - インターネット等との接続による、情報システムと統合化
 - ITSなどの高度交通システムへの対応による、交通インフラや他の車両と統合化
 - 他産業との連携したシステム開発
 - 住宅産業、電力産業、家電産業、情報サービス産業など
- 全体システムとしての安全性・信頼性の確保
 - 共通モデルによる上流段階での検証 など

■ 開発拠点のグローバル化

- リーマンショック後の円高に対応するため開発拠点の海外展開が進行
 - プラザ合意以降の円高に対応して生産拠点については海外展開が進行した(自動車産業では約4割が海外生産)
 - 2008年度までの国内組込みソフトウェア技術者の不足(約10万人不足と言われた)に対応するため海外拠点での技術者確保、海外へのアウトソーシングが拡大した
 - 既に海外拠点が存在し、海外でのソフトウェア開発経験も積んでおり、開発拠点の海外展開を進める土壌はできている
 - 今後、国内の開発リソース需要は減少(特に、ソフトウェア実装・テストの外部委託は、海外移転と自動化などにより国内市場は消滅)
- 国内組込みソフトウェア産業の構造改革が急務

ソフトウェア品質監査制度(仮称)検討の背景と経緯

第三者の検証・妥当性確認による品質説明力強化の必要性

品質説明に対する市場意識の変化

品質説明力の不足：当事者企業の技術的主張だけでなく、第三者の裏付け(検証、妥当性確認)による品質説明への要求の増大

製品と利用者とのギャップの拡大

利用品質低下の懸念：製品・システムの高度化・複雑化と利用者の多様化により、製品・システムと利用者との間のギャップが拡大

先端技術製品の潜在リスクへの不安

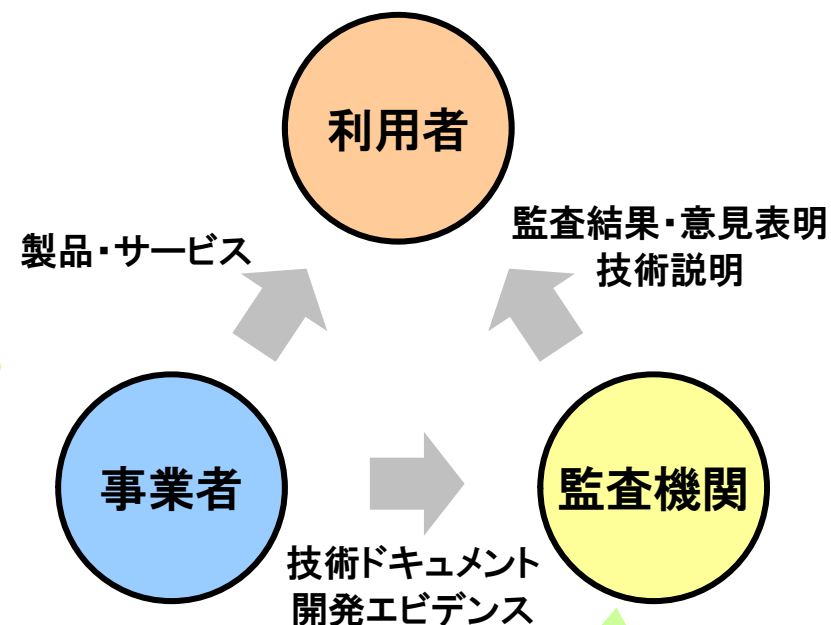
製品品質低下の懸念：技術の急速な進歩により技術標準(規格)に基づく規格認証の対象範囲外となる領域が拡大

品質文化の異なる業界を跨るシステム

残存する潜在リスクの増加：複数の業界を跨るシステムの拡大に伴い、全体システムとしての品質確認の精度が低下

IPA/SECでの活動経緯

- 2010年3月：産構審情報システム・ソフトウェア小委員会にて第三者による検証・妥当性確認の枠組みの必要性が示される
- 2010年4月：IPA/SECの統合系プロジェクト内に検討チームを発足
- 2010年7月：調査活動開始
- 2010年11月：制度検討委員会発足(主査：名古屋大学高田教授)
- 2011年6月：中間報告



第三者による検証・妥当性確認

事業者の技術的主張の妥当性を、監査機関が開発技術水準と利用技術水準を考慮して第三者の立場で評価し、技術に関する専門知識のない利用者にも理解できる形で情報提供する仕組み

(会計処理における会計監査と同等の役割)

ソフトウェア品質監査制度(仮称)の狙いと効果

国民生活の安全・安心・快適の向上と我が国産業の国際競争力の強化

ソフトウェア品質監査制度(仮称)の狙い

企業の製品・システムに関する利用者や市場への品質説明力の強化

国際市場における日本製品・システムの品質に対する正当な評価の確立

産業界の枠を超えた品質の見える化による複数の産業界を跨り構成される高度なシステムの開発加速（例：スマートコミュニティシステムなど）

製品・システムの本質的な品質向上

ソフトウェア品質監査制度(仮称)の効果

技術の専門家ではない**利用者の安心感の向上**

我が国産業の**国際競争力の維持・強化**

国民生活の快適性・利便性の向上

新成長戦略分野における我が国産業の**国際優位性の確保**

国民生活の安全性の確保

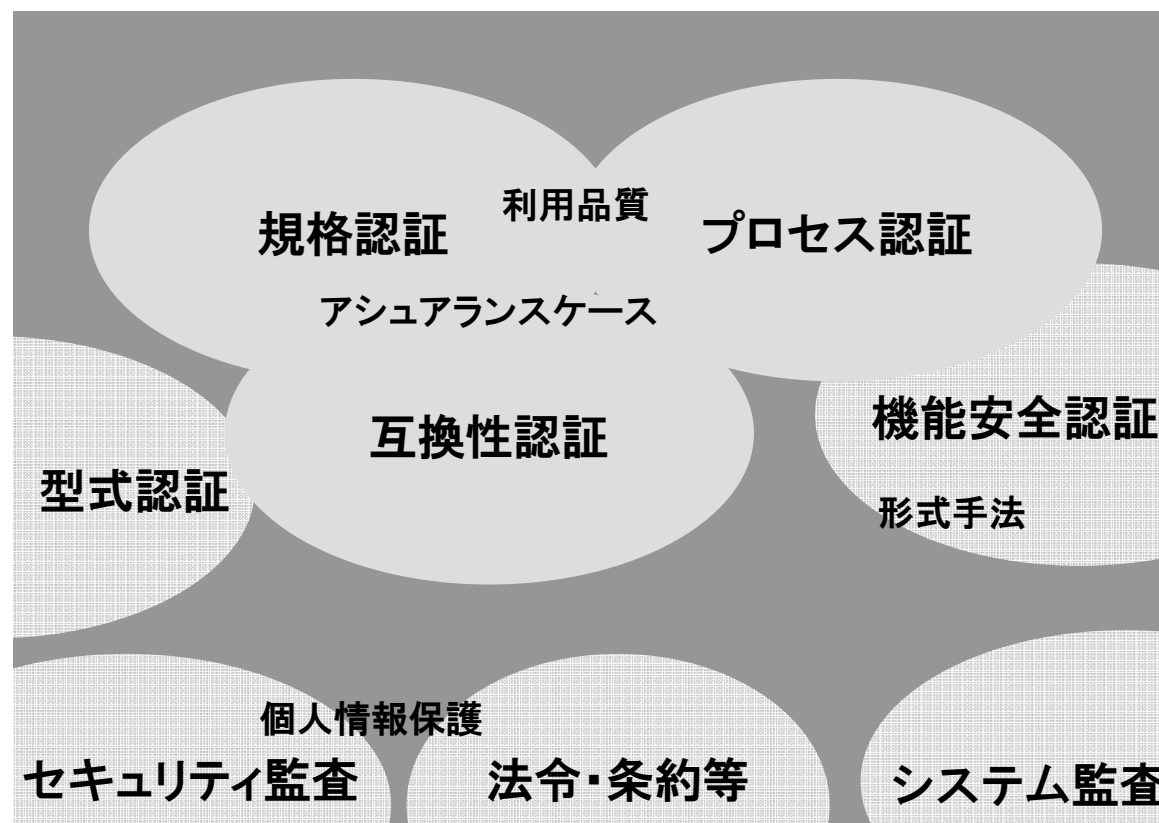
ご参考：米国の状況

- 2010年日本製自動車の制御システムに対する不具合の疑念が拡大。米国政府の要請で、NASAの独立検証・妥当性確認(IV&V)センターが第三者の立場で、制御システムの検証ならびに妥当性確認を実施。2011年2月、不具合が発見されなかったとの最終報告が公開。
- 当事者企業の主張だけでなく、第三者の主張がないと説明力が不十分との意識（会計処理における会計監査の必要性和同等の意識）。
- 国防省やNASAのシステムの調達、航空機分野、医療機器分野で類似した仕組みを運用している。

ソフトウェア品質監査制度(仮称)の特長

- 独立検証機関による検証と妥当性確認を包含
 - 事業者の主張を高度な専門技術を持った独立検証機関で再確認
- 利用情報や利用者情報に基づく利用品質の確認
 - すべての開発ライフサイクルでの利用情報、利用者情報の活用を確認
- 既存の認証制度や監査制度を補完
 - 既存の認証結果・監査結果を確認し、重複した監査を簡略化
- 開発ライフサイクルに合わせて開発と並行して監査を実施
 - 指摘事項への対応による手戻りが防止でき、出荷時期等への影響を最小化
- 機密情報の拡散リスクを低減できる内部審査官と外部審査官が連携
 - 外部審査官の管理下で内部審査官が機密情報を直接アクセスする監査業務を実施

利用者・市場が期待する第三者による確認範囲



- ソフトウェア品質監査制度(仮称)で監査する範囲
- 他の認証・監査の結果を確認する範囲

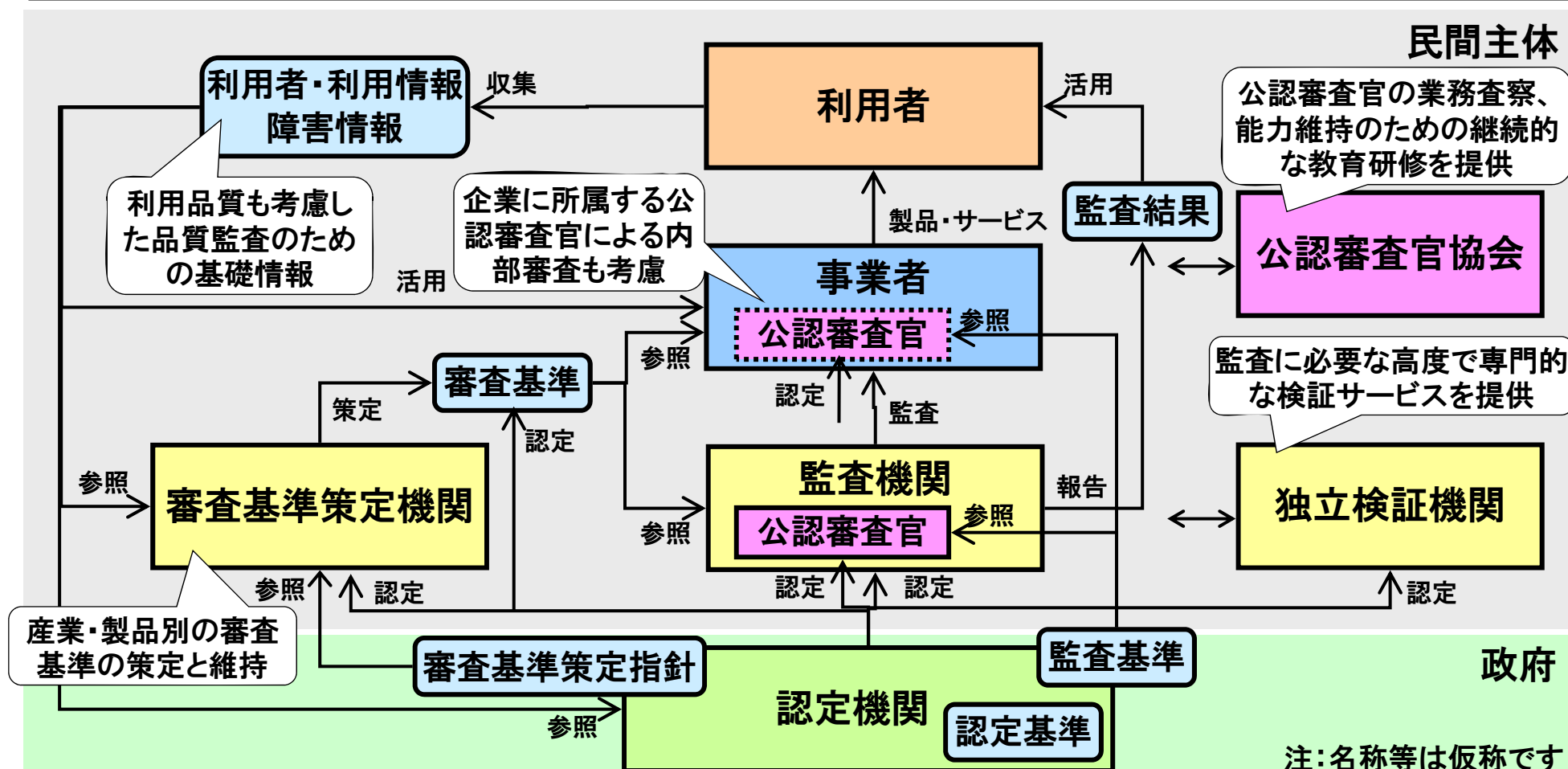
ソフトウェア品質監査制度(仮称)の枠組み

産業・製品分野別への対応と内部監査を考慮したフレームワーク

下記の要件を満たす「公認審査官」が、産業分野あるいは製品分野毎に定められた「審査基準」を基に、「監査基準」に従って監査業務を遂行し、「監査結果」を利用者にも理解できる形で情報提供する制度

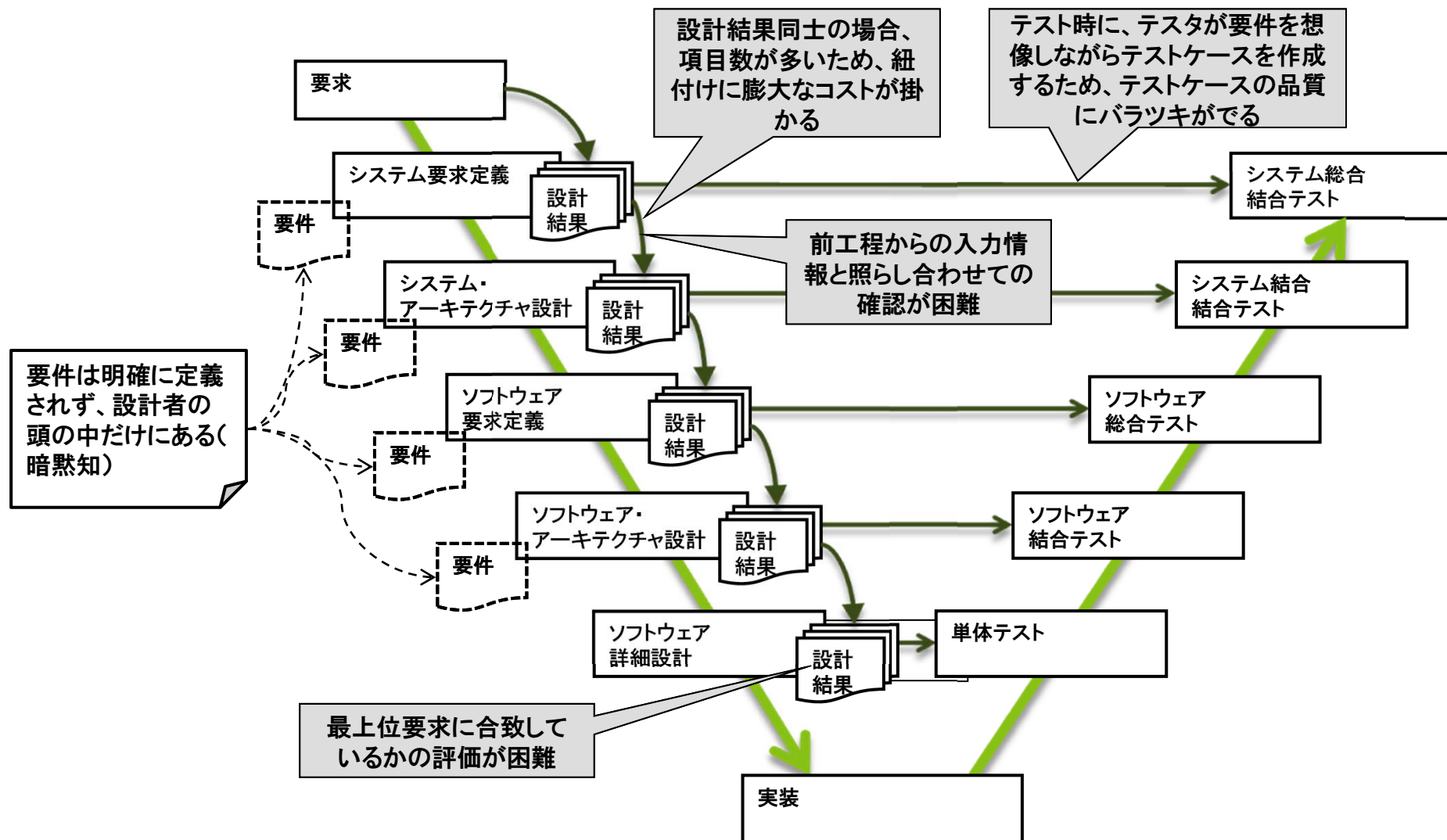
要件1. 専門性: 情報の信頼性を保証できる専門知識と能力を有していること

要件2. 独立性: 監査対象の事業者・利用者から身分的・経済的・精神的に独立していること



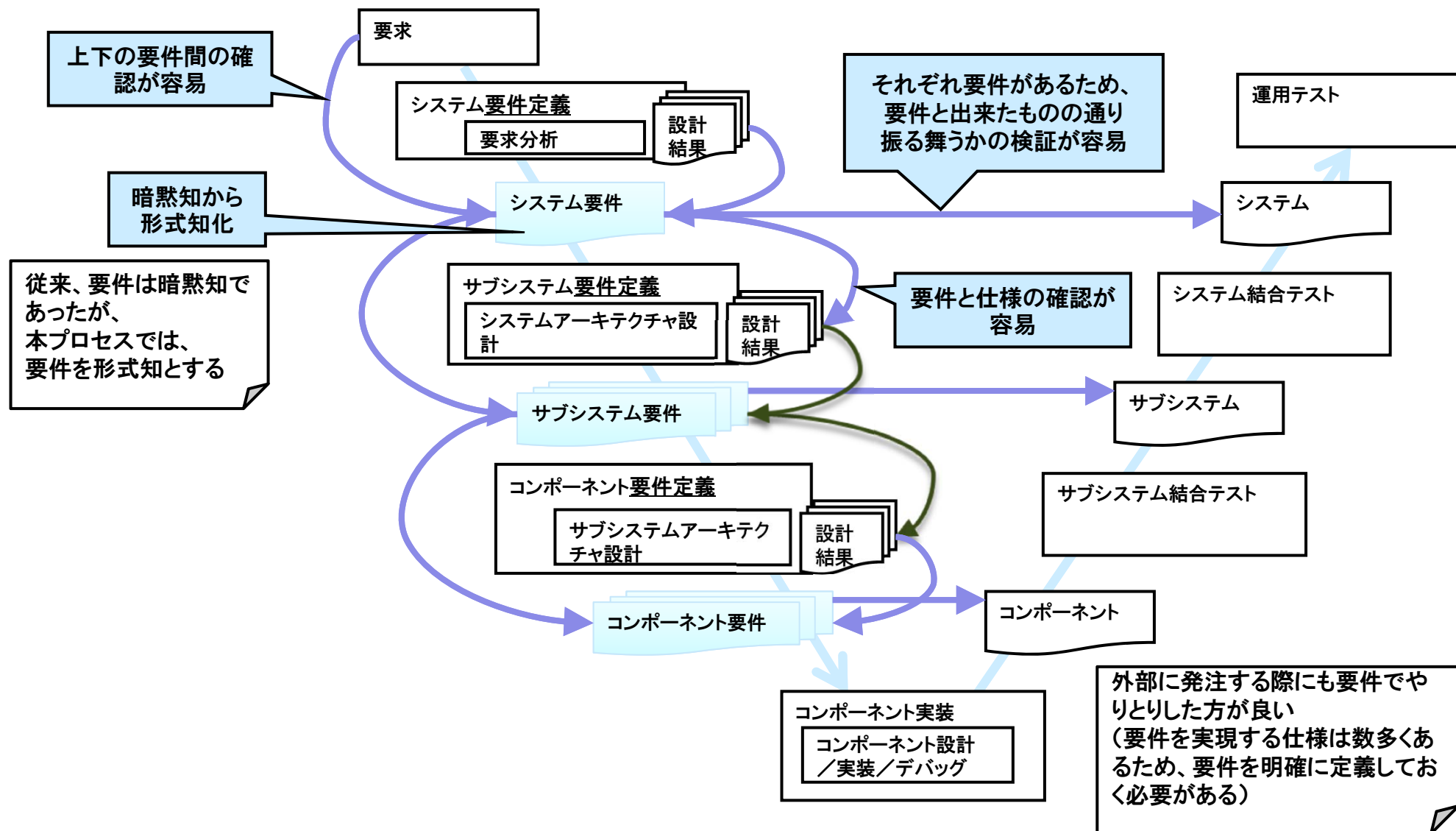
従来型開発プロセス(仕様ベース)のソフトウェア品質監査における課題

大規模ソフトウェアではソフトウェア開発工程も階層化されるが工程間は仕様で受渡し



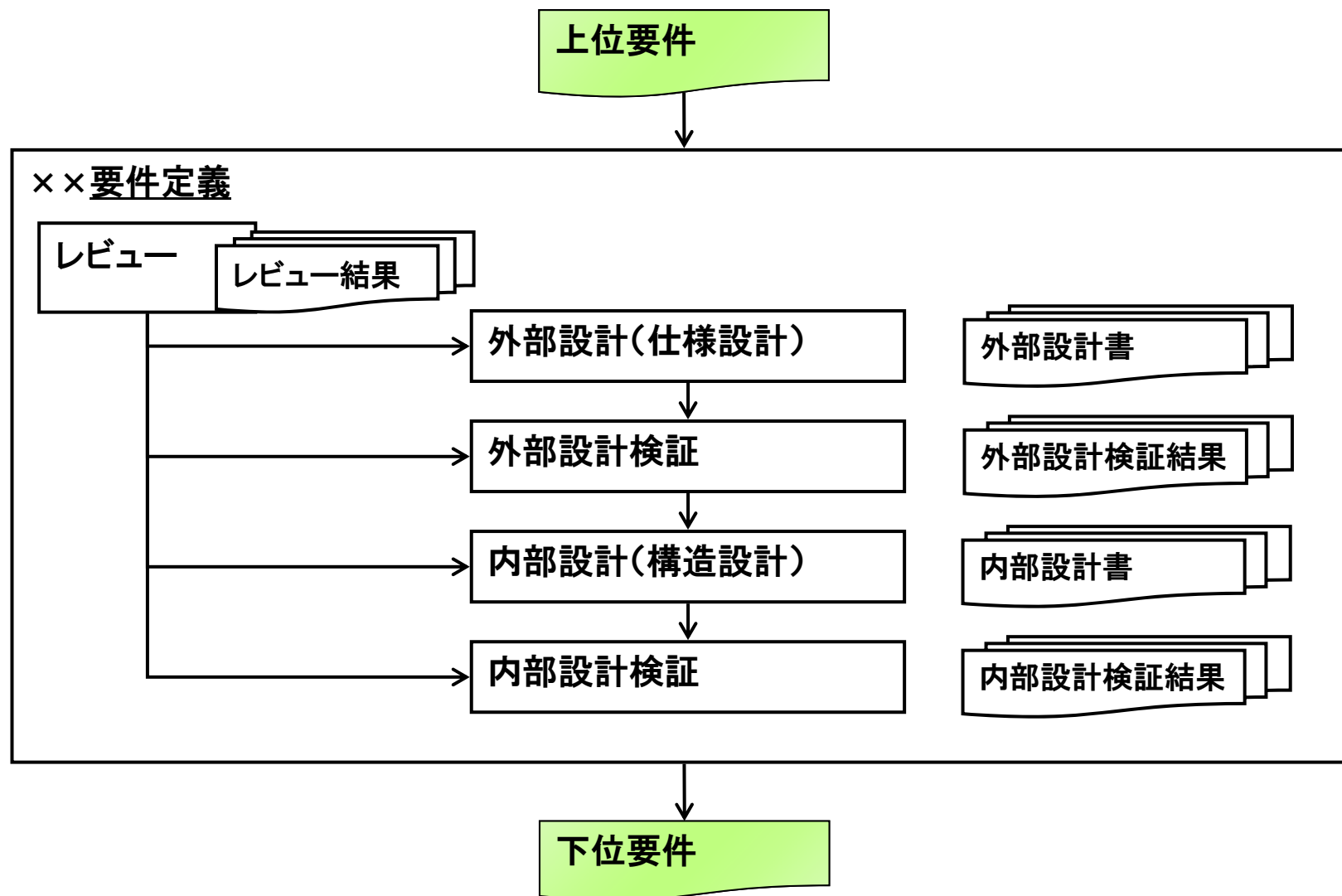
ソフトウェア品質監査を効率的に実施できる開発プロセス(要件ベース)

階層化されるソフトウェア開発工程を要件で受渡し



要件ベース開発プロセスの各要件定義工程のタスクモデル

外部設計、内部設計(構造設計)、下位要件の検証・妥当性確認を工程内で閉じて実施可能



ご参考：米連邦航空局製品認証における開発プロセスARP4754A(Guidelines for Development of Civil Aircraft and Systems)

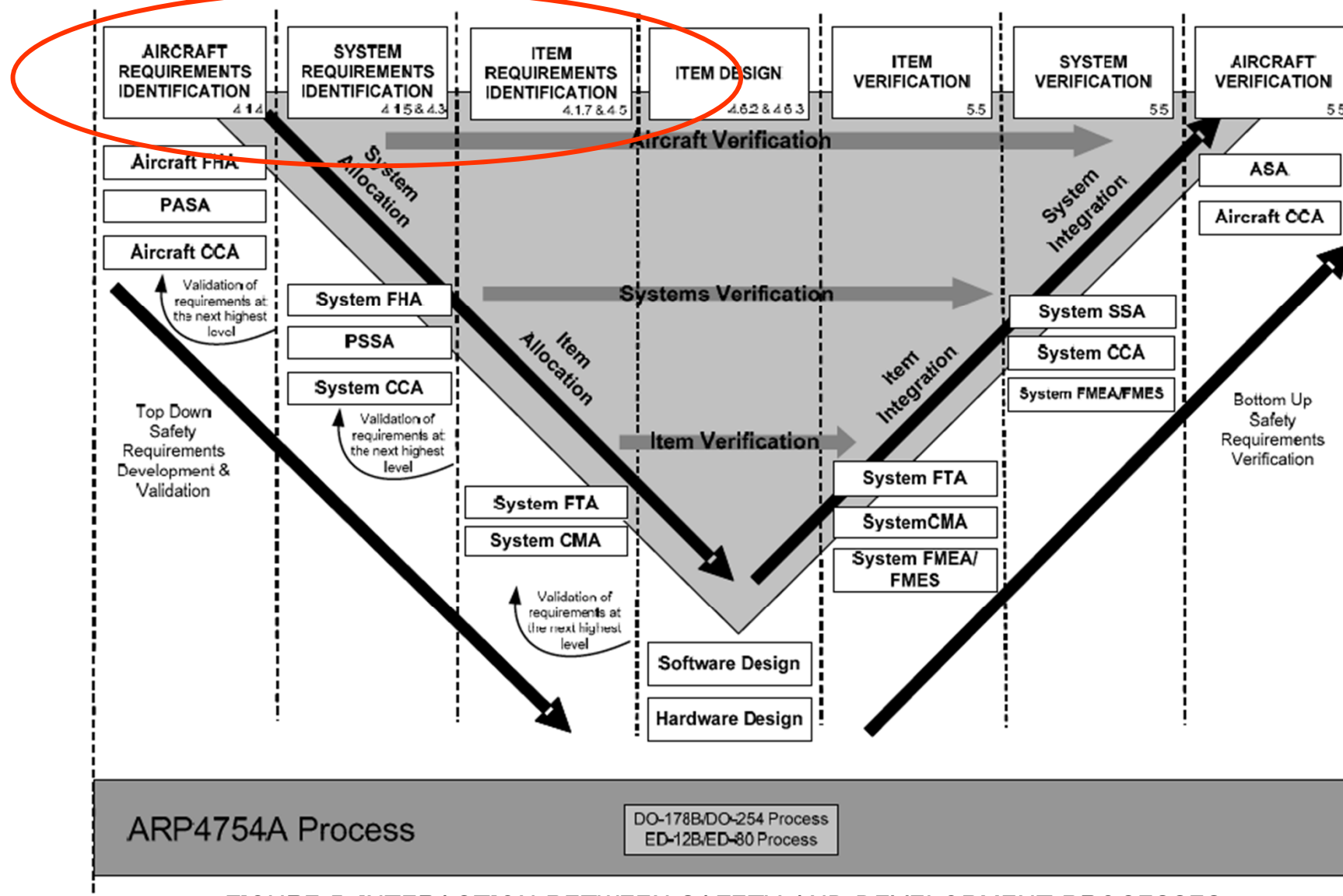
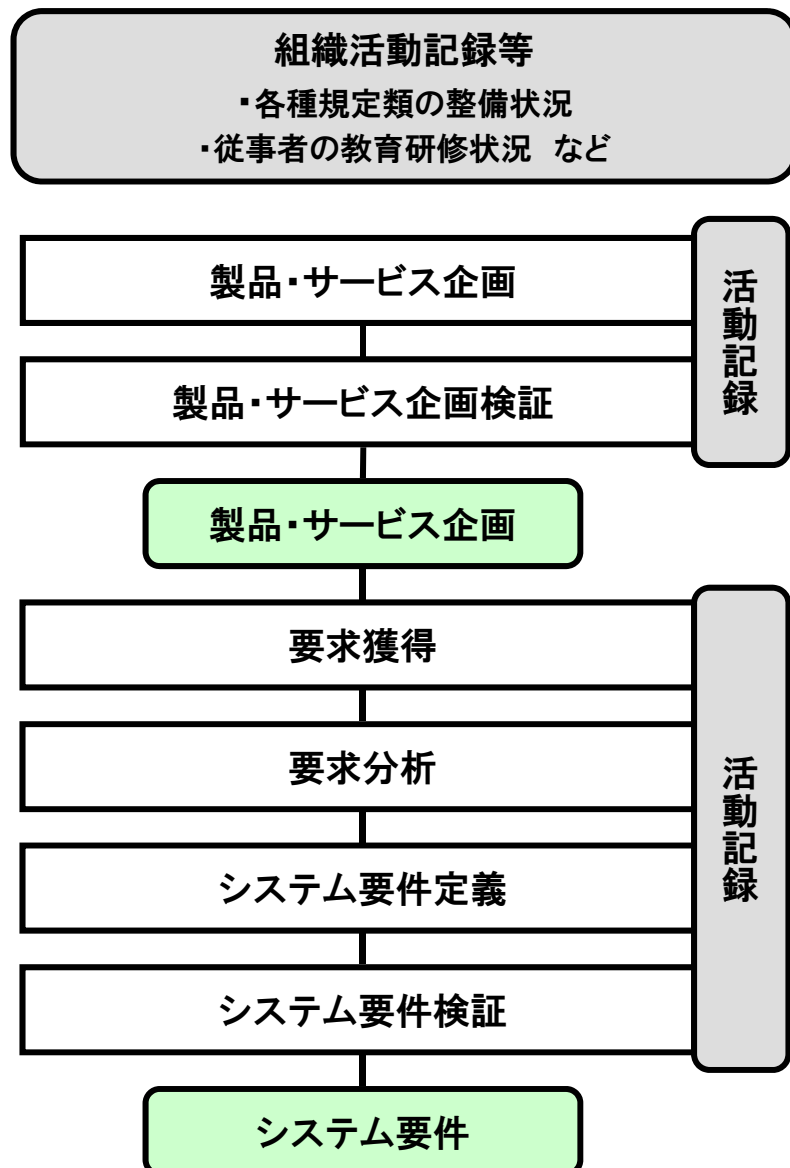


FIGURE 5-INTERACTION BETWEEN SAFETY AND DEVELOPMENT PROCESSES

出典：SAE
ARP4754A

製品・システムのライフサイクル毎のソフトウェア品質監査(仮称)の業務

製品・サービスの企画からシステム要件まで

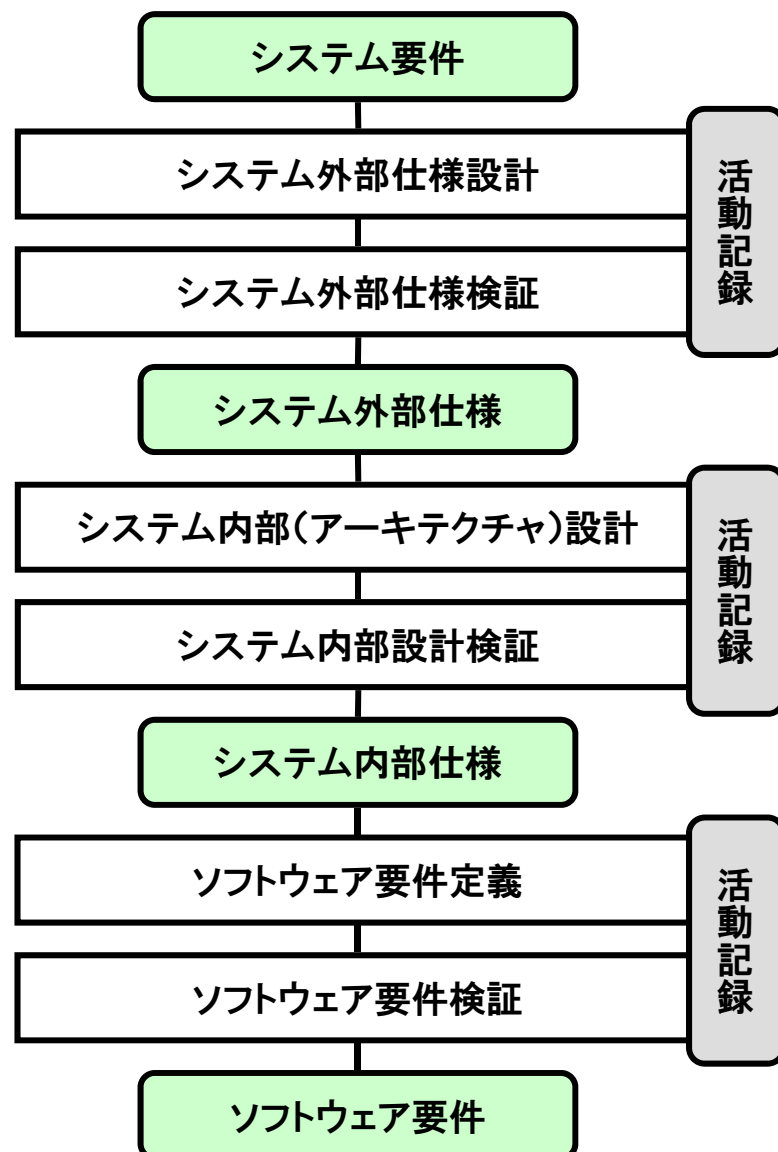


- ・製品・サービスの企画が妥当か
- ・製品・サービスに関連する規定類は妥当か
- ・製品・サービスに関わる従事者は妥当か

- ・システム要件は製品・サービスの企画と整合しているか
- ・要求獲得は妥当か
- ・要求分析は妥当か
- ・システム要件の検証は妥当か
- ・システム要件は妥当か

製品・システムのライフサイクル毎のソフトウェア品質監査(仮称)の業務

システム要件からソフトウェア要件まで



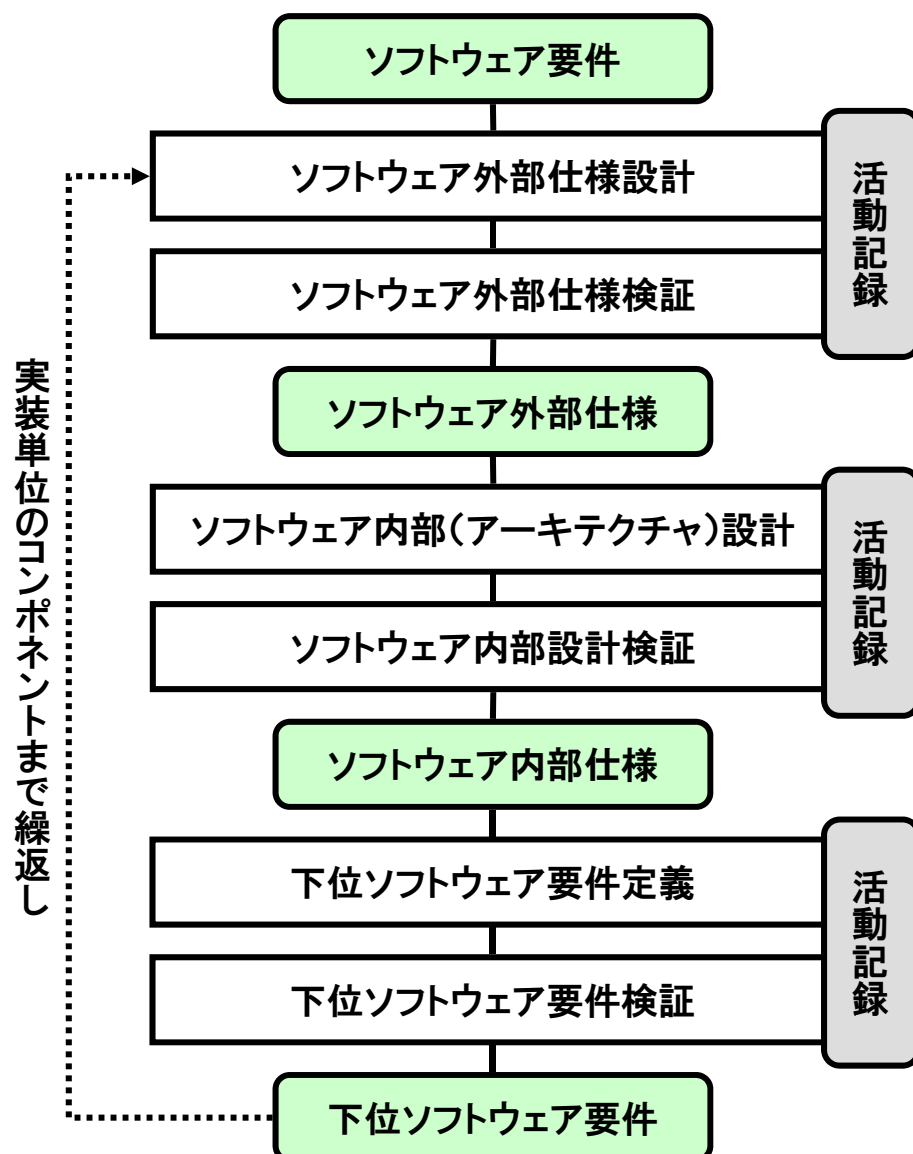
- ・システム外部仕様はシステム要件を満たしているか
- ・システム外部設計の検証は妥当か
- ・システム外部仕様は妥当か

- ・システム内部仕様はシステム外部仕様と整合しているか
- ・システム内部設計の検証は妥当か
- ・システム内部仕様は妥当か

- ・ソフトウェア要件はシステム内部仕様と整合しているか
- ・ソフトウェア要件の検証は妥当か
- ・ソフトウェア要件はシステム要件を満足しているか
- ・ソフトウェア要件は妥当か

製品・システムのライフサイクル毎のソフトウェア品質監査(仮称)の業務

ソフトウェア要件から下位ソフトウェア要件まで



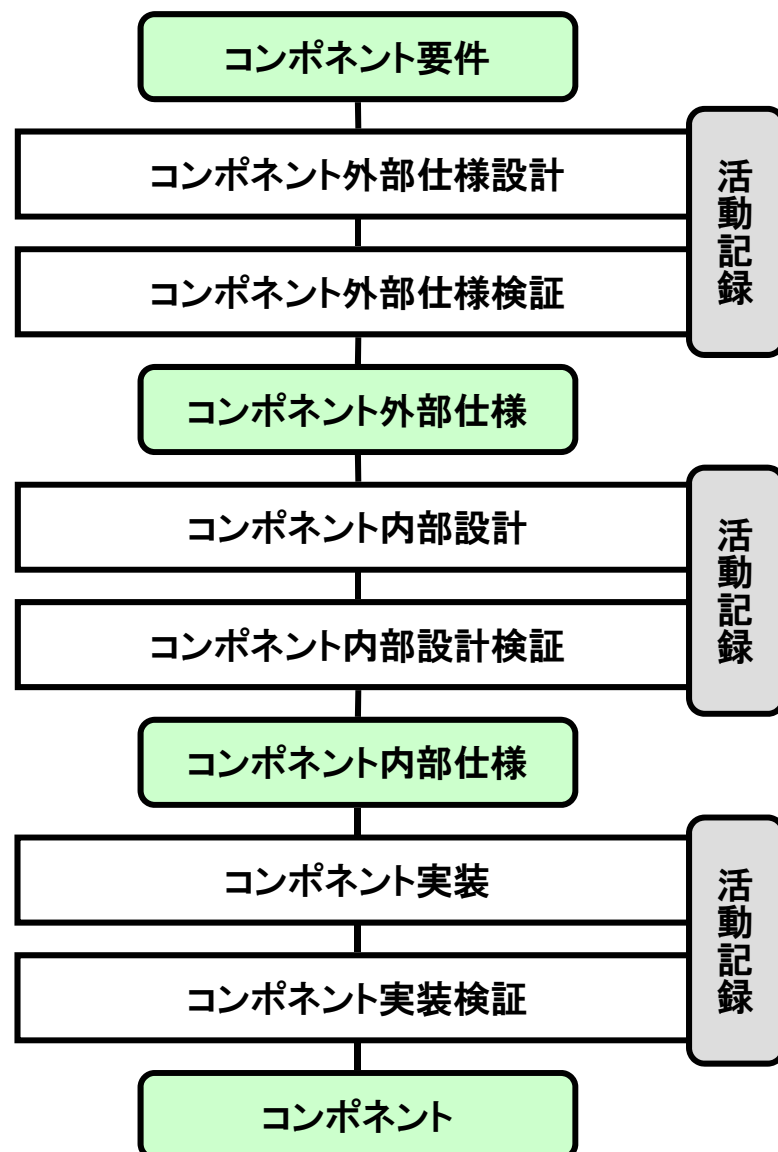
- ・ソフトウェア外部仕様はソフトウェア要件を満たしているか
- ・ソフトウェア外部設計の検証は妥当か
- ・ソフトウェア外部仕様は妥当か

- ・ソフトウェア内部仕様はソフトウェア外部仕様と整合しているか
- ・ソフトウェア内部設計の検証は妥当か
- ・ソフトウェア内部仕様は妥当か

- ・下位ソフトウェア要件はソフトウェア内部仕様と整合しているか
- ・下位ソフトウェア要件の検証は妥当か
- ・下位ソフトウェア要件はソフトウェア要件を満たしているか
- ・下位ソフトウェア要件は妥当か

製品・システムのライフサイクル毎のソフトウェア品質監査(仮称)の業務

コンポーネント(実装単位となるソフトウェア部分)要件からコンポーネントまで

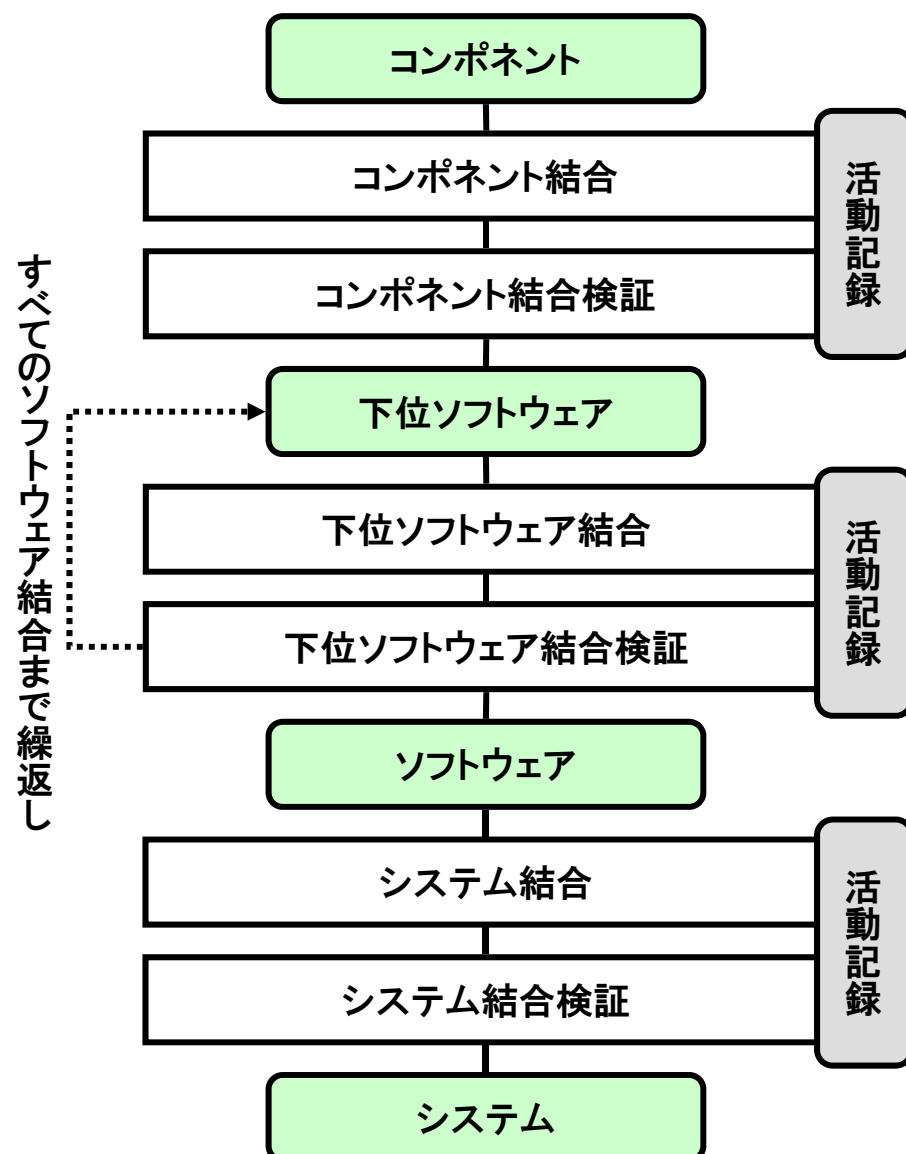


- ・コンポーネント外部仕様はコンポーネント要件を満たしているか
- ・コンポーネント外部設計の検証は妥当か
- ・コンポーネント外部仕様は妥当か

- ・コンポーネント内部仕様はコンポーネント外部仕様と整合しているか
- ・コンポーネント内部設計の検証は妥当か
- ・コンポーネント内部仕様は妥当か

- ・コンポーネント実装はコンポーネント内部仕様と整合しているか
- ・コンポーネント実装の検証は妥当か
- ・コンポーネント実装はコンポーネント要件を満足しているか
- ・コンポーネント実装は妥当か

製品・システムのライフサイクル毎のソフトウェア品質監査(仮称)の業務 コンポーネントからシステムまで

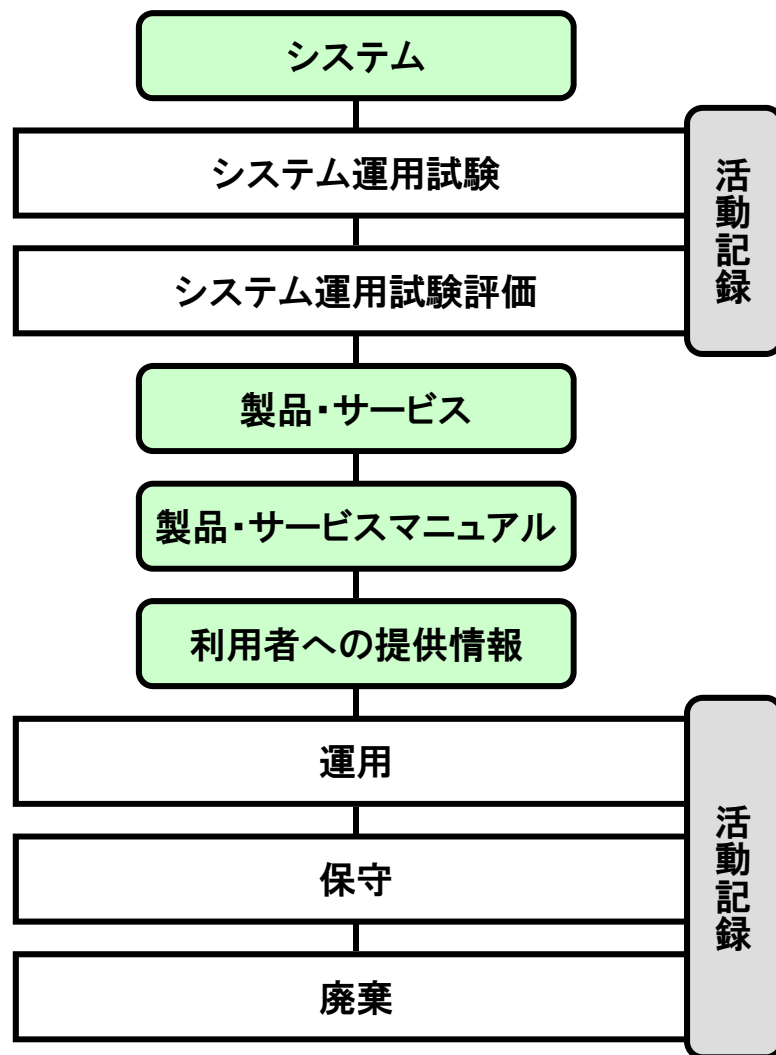


- ・コンポーネント結合は妥当か
- ・コンポーネント結合の検証は妥当か
- ・結合された下位ソフトウェアは下位ソフトウェア要件を満足しているか

- ・下位ソフトウェア結合は妥当か
- ・下位ソフトウェア結合の検証は妥当か
- ・結合されたソフトウェアはソフトウェア要件を満たしているか

- ・システム結合は妥当か
- ・システム結合の検証は妥当か
- ・結合されたシステムはシステム要件を満たしているか

製品・システムのライフサイクル毎のソフトウェア品質監査(仮称)の業務 システムから廃棄まで



- ・システム運用試験は妥当か
- ・システム運用試験の評価は妥当か
- ・システムは企画を満足しているか

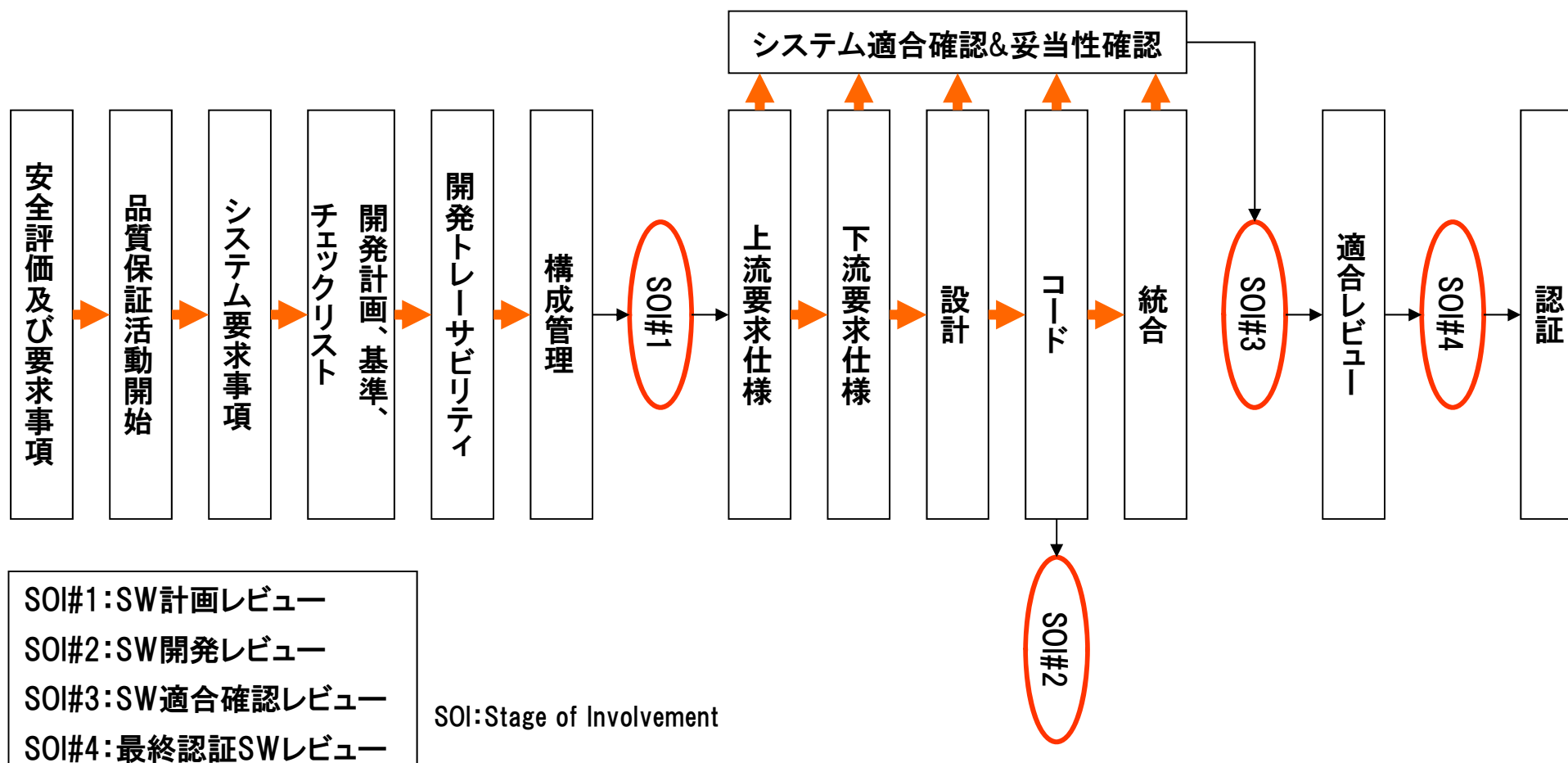
- ・製品・サービスのマニュアルは製品・サービスと整合しているか
- ・製品・サービスのマニュアルは妥当か
- ・利用者への提供情報は妥当か

- ・製品・サービスの運用は妥当か
- ・製品・サービスの保守は妥当か
- ・製品・サービスの廃棄は妥当か

ご参考：米連邦航空局製品認証におけるDERのレビュータイミング

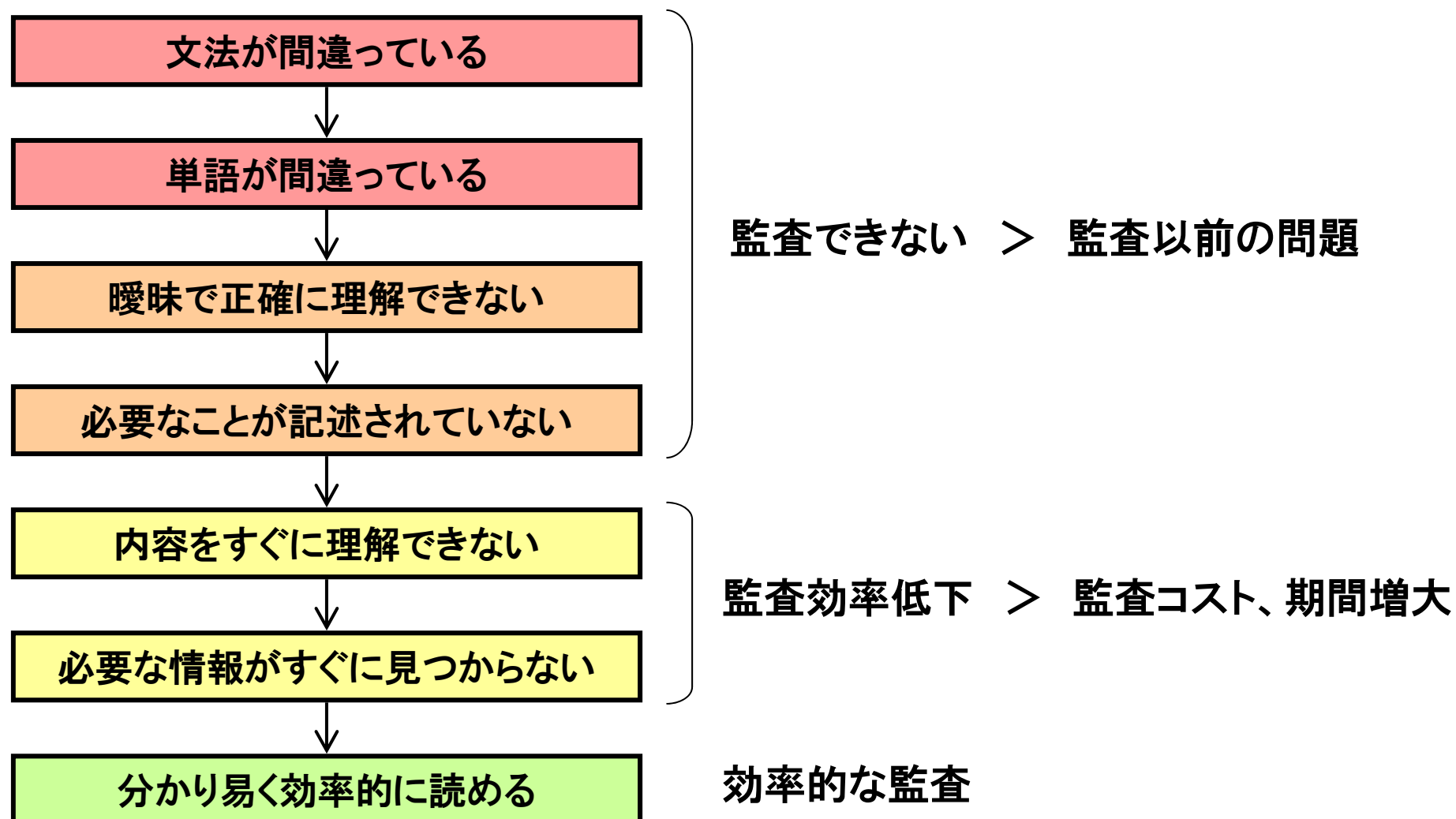
- DERの公式レビューは以下に示した「D0-178Bソフトウェア認証プロセス」のSOI#1、SOI#2、SOI#3、SOI#4のタイミングで実施
- DERは上記の4つの**公式レビュー**の他に、以下のプロセスの ➡ の14のタイミングで**机上レビュー**を実施

D0-178Bソフトウェア認証プロセス

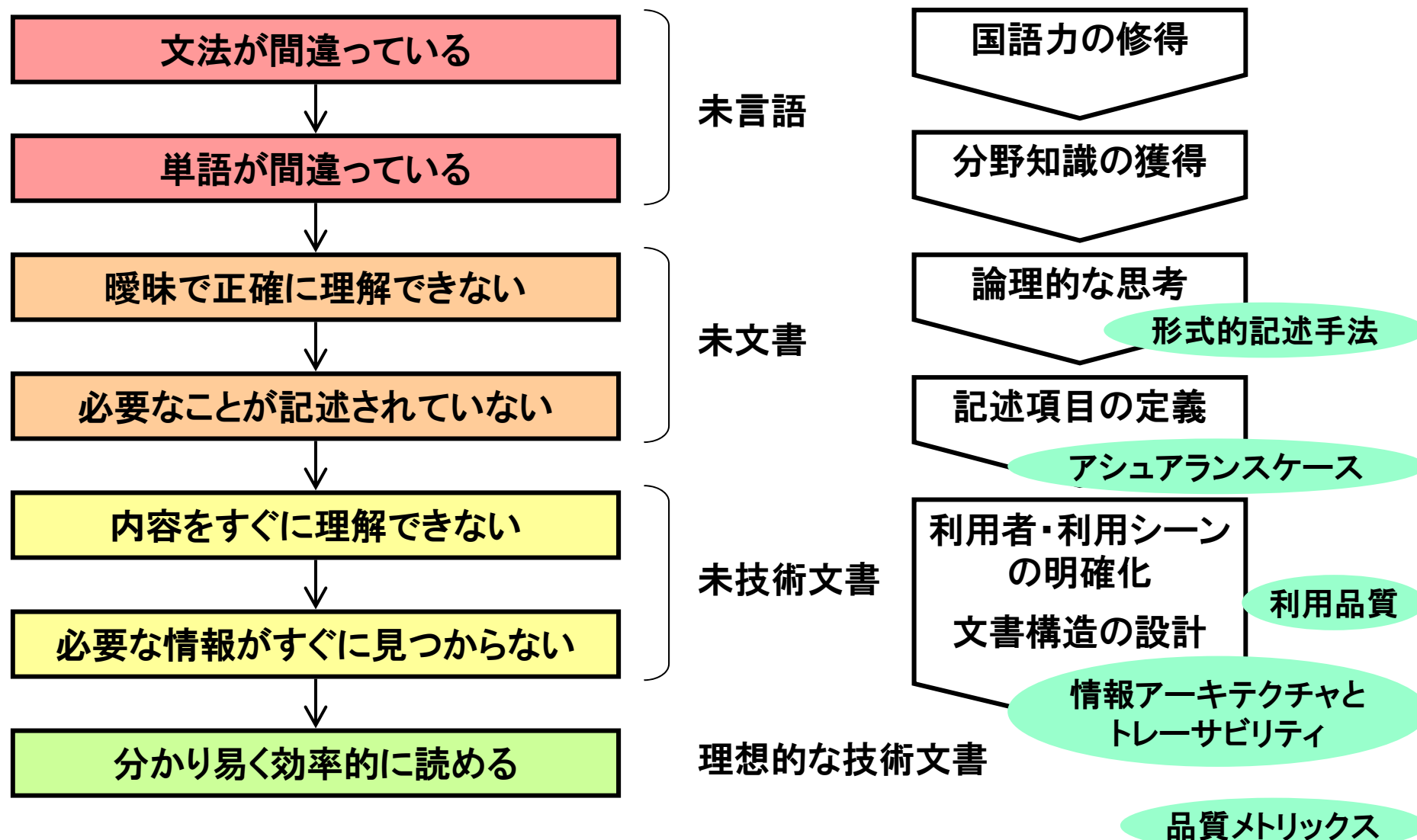


品質監査と技術ドキュメント/開発エビデンスの品質

- ソフトウェア品質監査 ≡ 技術ドキュメント/開発エビデンスを精査し妥当性を確認

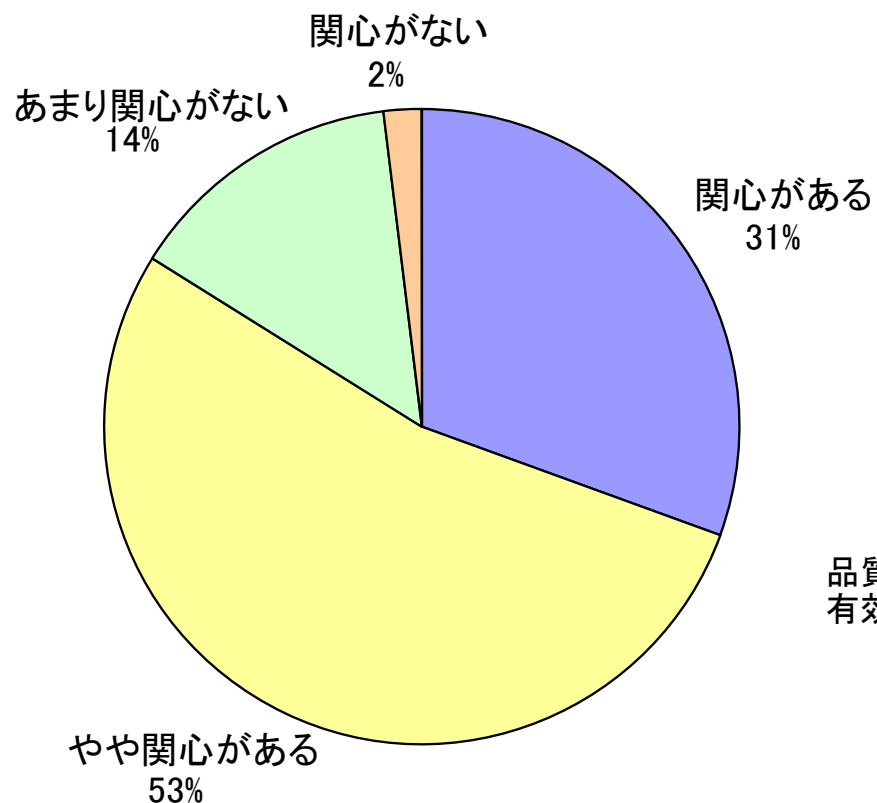


技術ドキュメント/開発エビデンスの高品質化に向けて

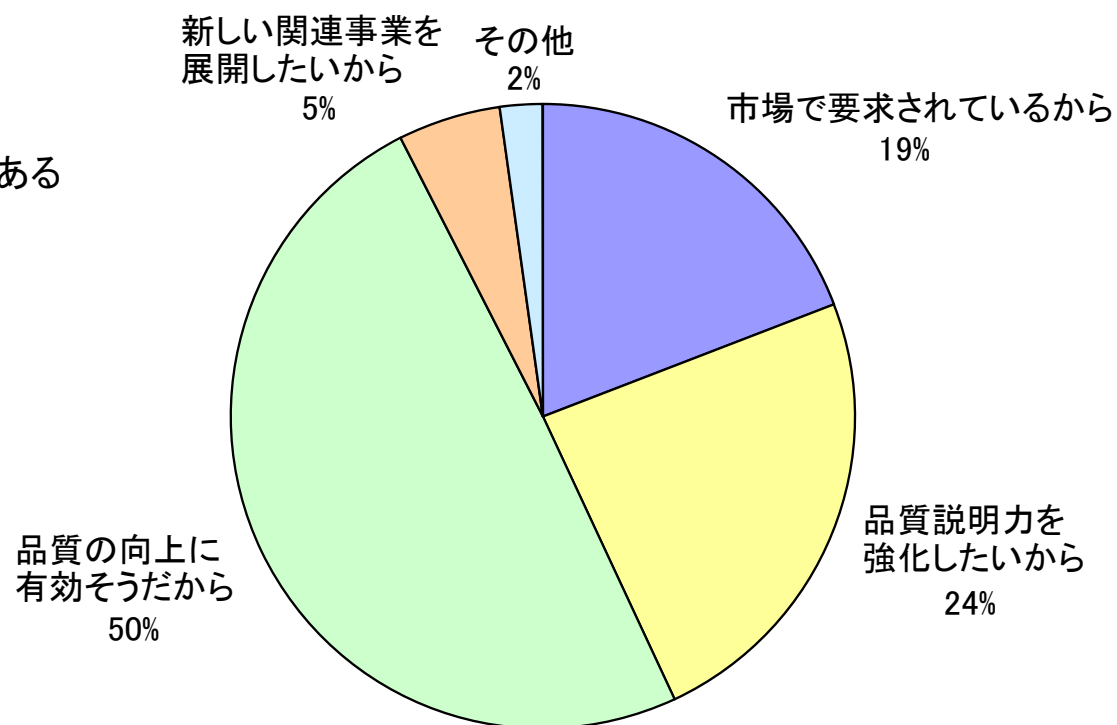


ESEC(2011年5月)のIPA/SECブース来場者へのアンケート結果

品質監査制度(仮称)に関心がありますか？
(回答数:2154名)



どのような観点で関心がありますか？
(回答数:1985名)



ご清聴ありがとうございました